IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

CRYSTAL LEE, individually and on behalf of all others similarly situated,	)	
Plaintiff,	)	Case No.:
v.	)	
INSIDER, INC.,	)	
Defendant.	)	

CLASS ACTION COMPLAINT

Plaintiff Crystal Lee ("Plaintiff"), individually and on behalf of all others similarly situated, hereby files this Class Action Complaint against Defendant Insider, Inc. ("Defendant" or "Insider"), and in support thereof alleges the following:

INTRODUCTION

1. This is a class action brought against Insider, an American online media company known for publishing the financial news website Insider, Business Insider, and other news and media websites, for surreptitiously intercepting the private electronic communications of visitors to its websites without consent.

2. Defendant knowingly directs third-party vendors, such as Microsoft Corporation, to embed snippets of JavaScript computer code ("Session Replay Code") on Defendant's websites, which then deploys on each website visitor's internet browser for the purpose intercepting and recording the website visitor's private electronic communications with the Defendant's websites, including their mouse movements, clicks, keystrokes (such as text being entered into an information field or text box), URLs of web pages visited, and/or other electronic communications

in real-time ("Website Communications"). These third-party vendors (collectively, "Session Replay Providers") create and deploy the Session Replay Code at Defendant's request.

3. After intercepting and recording the Website Communications, Defendant and the Session Replay Providers use those Website Communications to recreate website visitors' entire visit to Defendant's websites. The Session Replay Providers create a video replay of the user's behavior on the website and provide it to Defendant for analysis. Defendant's directive to the Session Replay Providers to secretly deploy the Session Replay Code results in the electronic equivalent of "looking over the shoulder" of each visitor to the Defendant website for the entire duration of their website interaction.

4. Defendant's conduct violates the Illinois Eavesdropping Act, 720 ILCS 5/14-1, *et seq.* and constitutes an invasion of the privacy rights of website visitors.

5. Plaintiff brings this action individually and on behalf of a class of all Illinois citizens whose Website Communications were intercepted at Defendant's direction and use of Session Replay Code embedded on the webpages owned or controlled by Defendant and seeks all civil remedies provided under the causes of action, including but not limited to compensatory, statutory, and/or punitive damages, and attorneys' fees and costs.

PARTIES

Plaintiff Crystal Lee

6. Plaintiff Crystal Lee is a citizen of the State of Illinois, and at all times relevant to this action, resided and was domiciled in Illinois. Plaintiff is a citizen of Illinois.

Defendant Insider, Inc.

7. Defendant Insider, Inc. is Delaware Corporation with a principal place of business in New York, New York.

JURISDICTION AND VENUE

8. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d)(2)(A) because this case is a class action where the aggregate claims of all members of the proposed class are in excess of $5,000,000.00, exclusive of interest and costs, there are 100 or more members of the proposed class, and at least one member of the proposed class, including the Plaintiff, who is a citizen of a state (Illinois) different than Defendant (Delaware and/or New York).

9. This Court has personal jurisdiction over Defendant because a substantial part of the events and conduct giving rise to Plaintiff's claims occurred in Illinois. The privacy violations complained of herein resulted from Defendant's purposeful and tortious acts directed towards citizens of Illinois while they were located within Illinois. At all relevant times, Defendant knew that its practices would directly result in collection of information from Illinois citizens while those citizens browse Defendant's web properties. Defendant chose to avail itself of the business opportunities in Illinois by collecting real-time data from website visit sessions initiated by Illinoisans while located in Illinois, and the claims alleged herein arise from those activities.

10. Pursuant to 28 U.S.C. § 1391, this Court is the proper venue for this action because a substantial part of the events, omissions, and acts giving rise to the claims herein occurred in this District.

FACTUAL ALLEGATIONS

A. Website User and Usage Data Have Immense Economic Value.

11. The "world's most valuable resource is no longer oil, but data."[1]

[1] *The world's most valuable resource is no longer oil, but data*, The Economist (May 6, 2017), https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longeroil-but-data.

12. Earlier this year, Business News Daily reported that some businesses collect personal data (*i.e.*, gender, web browser cookies, IP addresses, and device IDs), engagement data (*i.e.*, how consumers interact with a business's website, applications, and emails), behavioral data (*i.e.*, customers' purchase histories and product usage information), and attitudinal data (*i.e.*, data on consumer satisfaction) from consumers.[2] This information is valuable to companies because they can use this data to improve customer experiences, refine their marketing strategies, capture data to sell it, and even to secure more sensitive consumer data.[3]

13. In a consumer-driven world, the ability to capture and use customer data to shape products, solutions, and the buying experience is critically important to a business's success. Research shows that organizations who "leverage customer behavior insights outperform peers by 85 percent in sales growth and more than 25 percent in gross margin."[4]

14. In 2013, the Organization for Economic Cooperation and Development ("OECD") even published a paper entitled "Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value."[5] In this paper, the OECD measured prices demanded by companies concerning user data derived from "various online data warehouses."[6]

15. OECD indicated that "[a]t the time of writing, the following elements of personal data were available for various prices: USD 0.50 cents for an address, USD 2 [i.e. $2] for a date

---

[2] Max Freedman, *How Businesses Are Collecting Data (And What They're Doing With It)*, Business News Daily (Aug. 5, 2022), https://www.businessnewsdaily.com/10625-businesses- collecting-data.html.
[3] *Id*.
[4] Brad Brown, Kumar Kanagasabai, Prashant Pant & Goncalo Serpa Pinto, *Capturing value from your customer data*, McKinsey (Mar. 15, 2017), https://www.mckinsey.com/business-functions/quantumblack/our-insights/capturing-value-from-your-customer-data.
[5] Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value, OECD Digital Economy Papers, NO. 220 (Apr. 2, 2013), https://www.oecdilibrary.org/docserver/5k486qtxldmq-en.pdf.
[6] *Id*. at 25.

of birth, USD 8 for a social security number (government ID number), USD 3 for a driver's license number and USD 35 for a military record. A combination of address, date of birth, social security number, credit record and military is estimated to cost USD 55."[7]

B. Website Users Have a Reasonable Expectation of Privacy in Their Interactions with Websites.

16. Consumers are skeptical and are wary about their data being collected. A report released by KPMG shows that "a full 86% of the respondents said they feel a growing concern about data privacy, while 78% expressed fears about the amount of data being collected."[8]

17. Another recent paper also indicates that most website visitors will assume their detailed interactions with a website will only be used by the website and not be shared with a party they know nothing about.[9] As such, website visitors reasonably expect that their interactions with a website should not be released to third parties unless explicitly stated.[10]

18. Privacy polls and studies show that a majority of Americans consider one of the most important privacy rights to be the need for an individual's affirmative consent before a company collects and shares its customers' data.

19. A recent study by Consumer Reports shows that 92% of Americans believe that internet companies and websites should be required to obtain consent before selling or sharing

---

[7] *Id*.
[8] Lance Whitney, *Data privacy is a growing concern for more consumers*, TechRepublic (Aug. 17, 2021), https://www.techrepublic.com/article/data-privacy-is-a-growing-concern-for-more- consumers/.
[9] *CUJO AI Recent Survey Reveals U.S. Internet Users Expectations and Concerns Towards Privacy and Online Tracking*, CUJO (May 26, 2020), https://www.prnewswire.com/news-releases/cujo-ai-recent-survey-reveals-us-internet-users-expectations-and-concerns-towards-privacy-and-online-tracking-301064970.html.
[10] Frances S. Grodzinsky, Keith W. Miller & Marty J. Wolf, *Session Replay Scripts: A Privacy Analysis*, The Information Society, 38:4, 257, 258 (2022).

consumers' data, and the same percentage believe internet companies and websites should be required to provide consumers with a complete list of the data that has been collected about them.[11]

20. Moreover, according to a study by Pew Research Center, a majority of Americans, approximately 79%, are concerned about how data is collected about them by companies.[12]

21. Users act consistently with their expectation of privacy. Following a new rollout of the iPhone operating software – which asks users for clear, affirmative consent before allowing companies to track users – 85 percent of worldwide users and 94 percent of U.S. users chose not to allow such tracking.[13]

C. How Session Replay Code Works.

22. Session Replay Code, such as that implemented on www.Defendant.com, enables website operators to record, save, and replay website visitors' interactions with a given website. The clandestinely deployed code provides online marketers and website designers with insights into the user experience by recording website visitors "as they click, scroll, type or navigate across different web pages."[14]

---

[11] *Consumers Less Confident About Healthcare, Data Privacy, and Car Safety, New Survey Finds*, Consumer Reports (May 11, 2017), https://www.consumerreports.org/consumerreports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety/.

[12] *Americans and Privacy: Concerned, Confused, and Feeling Lack of Control Over Their Personal Information*, Pew Research Center, (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-Confusedand-feeling-lack-of-control-over-their-personal-information/.

[13] Margaret Taylor, *How Apple screwed Facebook*, Wired, (May 19, 2021), https://www.wired.co.uk/article/apple-ios14-facebook.

[14] Erin Gilliam Haije, *[Updated] Are Session Recording Tools a Risk to Internet Privacy?*, Mopinion (Mar. 7, 2018), https://mopinion.com/are-session-recording-tools-a-risk-to-internet- privacy/.

23. While Session Replay Code is utilized by websites for some legitimate purposes, it goes well beyond normal website analytics when it comes to collecting the actual contents of communications between website visitors and websites. Unlike other online advertising tools, Session Replay Code allows a website to capture and record nearly every action a website visitor takes while visiting the website, including actions that reveal the visitor's personal or private sensitive data, sometimes even when the visitor does not intend to submit the data to the website operator, or has not finished submitting the data to the website operator.[15] As a result, website visitors "aren't just sharing data with the [web]site they're on . . . but also with an analytics service that may be watching over their shoulder."[16]

24. Session Replay Code works by inserting computer code into the various event handling routines that web browsers use to receive input from users, thus intercepting the occurrence of actions the user takes. When a website delivers Session Replay Code to a user's browser, the browser will follow the code's instructions by sending responses in the form of "event" data to a designated third-party server. Typically, the server receiving the event data is controlled by the third-party entity that wrote the Session Replay Code, rather than the owner of the website where the code is installed.

25. The types of events captured by Session Replay Code vary by specific product and configuration, but in general are wide-ranging and can encompass virtually every user action, including all mouse movements, clicks, scrolls, zooms, window resizes, keystrokes, text entry, and numerous other forms of a user's navigation and interaction through the website. In order to permit

[15] *Id*.
[16] Eric Ravenscraft, *Almost Every Website You Visit Records Exactly How Your Mouse Moves*, Medium (Feb. 5, 2020), https://onezero.medium.com/almost-every-website-you-visit-records-exactly-how-your-mouse-moves-4134cb1cc7a0.

a reconstruction of a user's visit accurately, the Session Replay Code must be capable of capturing these events at hyper-frequent intervals, often just milliseconds apart. Events are typically accumulated and transmitted in blocks periodically throughout the user's website session, rather than after the user's visit to the website is completely finished.

26. Unless specifically masked through configurations chosen by the website owner, some visible contents of the website may also be transmitted to the Session Replay Provider.

27. Once the events from a user session have been recorded by a Session Replay Code, a website operator can view a visual reenactment of the user's visit through the Session Replay Provider, usually in the form of a video, meaning "[u]nlike typical analytics services that provide aggregate statistics, these scripts are intended for the recording and playback of individual browsing sessions."[17]

28. Because most Session Replay Codes will by default indiscriminately capture the maximum range of user-initiated events and content displayed by the website, researchers have found that a variety of highly sensitive information can be captured in event responses from website visitors, including medical conditions, credit card details, and other personal information displayed or entered on webpages.[18]

29. Most alarming, Session Replay Code may capture data that the user did not even intentionally transmit to a website during a visit, and then make that data available to website owners when they access the session replay through the Session Replay Provider. For example, if a user writes information into a text form field, but then chooses not to click a "submit" or "enter"

[17] Steven Englehardt, *No boundaries: Exfiltration of personal data by session-replay scripts*, Freedom to Tinker (Nov. 15, 2017), https://freedom-to-tinker.com/2017/11/15/no-boundaries-exfiltration-of-personal-data-by-session-replay-scripts/.
[18] *Id*.

button on the website, the Session Replay Code may nevertheless cause the non-submitted text to be sent to the designated event-response-receiving server before the user deletes the text or leaves the page. This information will then be viewable to the website owner when accessing the session replay through the Session Replay Provider.

30. Session Replay Code does not necessarily anonymize user sessions, either.

31. First, if a user's entry of personally identifying information is captured in an event response, that data will become known and visible to both the Session Replay Provider and the website owner.

32. Second, if a website displays user account information to a logged-in user, that content may be captured by Session Replay Code.

33. Third, some Session Replay Providers explicitly offer website owners cookie functionality that permits linking a session to an identified user, who may be personally identified if the website owner has associated the user with an email address or username.[19]

34. Session Replay Providers often create "fingerprints" that are unique to a particular user's combination of computer and browser settings, screen configuration, and other detectable information. The resulting fingerprint, which is often unique to a user and rarely changes, are collected across all sites that the Session Replay Provider monitors.

35. When a user eventually identifies themselves to one of these websites (such as by filling in a form), the provider can then associate the fingerprint with the user identity and can then back-reference all of that user's other web browsing across other websites previously visited,

[19] *Id.*; *see also FS.identify – Identifying users*, FullStory, https://help.fullstory.com/hc/en-us/articles/360020828113, (last visited Sep. 8, 2022).

including on websites where the user had intended to remain anonymous—even if the user explicitly indicated that they would like to remain anonymous by enabling private browsing.

36. In addition to the privacy invasions caused by the diversion of user communications with websites to third-party Session Replay Providers, Session Replay Code also exposes website visitors to identity theft, online scams, and other privacy threats.[20] Indeed, "[t]he more copies of sensitive information that exist, the broader the attack surface, and when data is being collected [] it may not be stored properly or have standard protections" increasing "the overall risk that data will someday publicly leak or be breached."[21]

37. Recognizing the privacy concerns posed by Session Replay Code, in 2019 Apple required app developers to remove or properly disclose the use of analytics code that allow app developers to record how a user interacts with their iPhone apps or face immediate removal from the app store.[22] In announcing this decision, Apple stated: "Protecting user privacy is paramount in the Apple ecosystem. Our App Store Review Guidelines require that apps request explicit user consent and provide a clear visual indication when recording, logging, or otherwise making a record of user activity."[23]

D. Defendant Secretly Eavesdrops on its Website Visitors' Electronic Communications.

[20] Juha Sarrinen, *Session Replay is a Major Threat to Privacy on the Web*, itnews (Nov. 16, 2017), https://www.itnews.com.au/news/session-replay-is-a-major-threat-to-privacy-on-the-web-477720.
[21] Lily Hay Newman, *Covert 'Replay Sessions' Have Been harvesting Passwords by Mistake*, WIRED (Feb. 26, 2018), https://www.wired.com/story/covert-replay-sessions-harvesting- passwords/.
[22] Zack Whittaker, *Apple Tells App Developers to Disclose or Remove Screen Recording Code*, TechCrunch (Feb. 7, 2019), https://techcrunch.com/2019/02/07/apple-glassbox-apps/.
[23] *Id*.

38. Defendant operates, at least, the websites www.insider.com and www.businessinsider.com.

39. Defendant's web properties are extremely popular. Upon information and belief, the web properties are visited by hundreds of millions of unique users monthly.

40. However, unbeknownst to the millions of individuals perusing Defendant's web properties, Defendant knowingly directs Session Replay Providers to embed various Session Replay Codes on its website to track and analyze website user interactions with Defendant's web properties. Because the Session Replay Providers are unknown eavesdroppers to visitors to Defendant's web properties, they are not parties to website visitors' Website Communications with Defendant.

41. Defendant knowingly derives a benefit and/or information from the Website Communications intercepted and recorded at its direction. Upon information and belief, Defendant uses the intercepted Website Communications to replay website visitors' interactions with its web properties, improve user interactions with its websites, and to gain and/or retain browsing data to further target advertisements to its website visitors.

42. Defendant's knowing direction and use of Session Replay Codes through various Session Replay Providers, and its knowing derivation of a benefit and/or information from the Website Communications surreptitiously intercepted and recorded by Session Replay Codes is a violation of Illinois statutory and common law.

E. Plaintiff's and Class Members' Experiences.

43. Plaintiff has independently visited at least one of Defendant's web properties while in Illinois on at least one occasion.

44. While visiting Defendant's website, Plaintiff fell victim to Defendant's unlawful monitoring, recording, and collection of Plaintiff's Website Communications with the web properties.

45. Unknown to Plaintiff, Defendant directs Session Replay Providers to embed Session Replay Code on its website or acts in concert with Session Replay Providers to ensure said code functions on the web properties.

46. During the website visit(s), Plaintiff's Website Communications were captured by Session Replay Code and sent to at least one Session Replay Provider.

47. The eavesdropping by the Session Replay Code is ongoing during the visit and they intercept the contents of these communications between Plaintiff and Defendant with instantaneous or near-instantaneous transmissions to the Session Replay Providers.

48. The Session Replay Codes operate in the same manner for all putative Class members.

49. Like Plaintiff, each Class member visited at least one of Defendant's web properties with Session Replay Code embedded in it, and Session Replay Codes intercepted the Class members' Website Communications with the web properties by sending hyper-frequent logs of those communications to Session Replay Providers.

50. Even if Defendant masks certain elements when it configures the settings of the Session Replay Code embedded on its websites, any operational iteration of the Session Replay Code will, by its very nature and purpose, intercept the contents of communications between the website's visitors and the website owner.

51. For example, even with heightened masking enabled, Session Replay Providers will still learn through the intercepted data exactly which pages a user navigates to, how the user moves

through the page (such as which areas the user clicks, zooms in on, or interacts with), and additional substantive information.

52. As a specific example, if a user types a particular string of text into the search bar and initiates a search, even if the text entered into the search bar is masked, Session Replay Providers will still learn what is entered into the bar as soon as the search result page loads. Upon information and belief, the string of text entered into the search bar is nearly instantaneously transmitted to This is so because the responsive search results will be displayed on the subsequent page, and the responsive content generated by Defendant will repeat the searched information back on the generated page. That information will not be masked even if user-inputted text is fully masked in a text field.

CLASS ACTION ALLEGATIONS

53. Plaintiff brings this action pursuant to Federal Rule of Civil Procedure 23 individually and on behalf of the following Class:

> All natural persons in the State of Illinois whose Website Communications were captured through the use of Session Replay Code embedded in one of Defendant's web properties.

54. Excluded from the class are Defendant, its parents, subsidiaries, affiliates, officers, and directors, all persons who make a timely election to be excluded from the class, the judge to whom this case is assigned and any immediate family members thereof, and the attorneys who enter their appearance in this action.

55. **Numerosity:** The members of the Class are so numerous that individual joinder of all Class members is impracticable. The precise number of Class members and their identities may be obtained from the books and records of Defendant or its Session Replay Providers.

56. **Commonality:** This action involves questions of law and fact that are common to the Class members. Such common questions include, but are not limited to:

(a) whether Defendant employed Session Replay Providers to intercept and record Defendant's website visitors' Website Communications;

(b) whether Defendant operated or participated in the operation of an eavesdropping device;

(c) whether Defendant derives a benefit or information from the illegal use of an eavesdropping device;

(d) whether Defendant directed another to use an eavesdropping device illegally on its behalf;

(e) whether Session Replay Code is an "eavesdropping device" used to intercept or record private electronic communications;

(f) whether Defendant acquired the contents of website users' private electronic communications without their consent;

(g) whether Plaintiff and Class members had a reasonable expectation of privacy in their Website communications;

(h) whether Defendant violated the Illinois Eavesdropping Act 720 ILCS 5/14- 1, *et seq.*;

(i) whether Plaintiff and the Class members are entitled to equitable relief; and

(j) whether Plaintiff and the Class members are entitled to actual, statutory, punitive, or other forms of damages, and other monetary relief.

57. **Typicality:** Plaintiff's claims are typical of the other Class members' claims because, among other things, all Class members were comparably injured through the uniform prohibited conduct described above. For instance, Plaintiff and each member of the Class had their electronic communications intercepted in violation of the law and their right to privacy. This uniform injury and the legal theories that underpin recovery make the claims of Plaintiff and the members of the Class typical of one another.

58. **Adequacy of Representation:** Plaintiff has and will continue to fairly and adequately represent and protect the interests of the Class. Plaintiff has retained counsel competent and experienced in complex litigation and class actions, including litigations to remedy privacy

violations. Plaintiff has no interest that is antagonistic to the interests of the Class, and Defendant has no defenses unique to any Plaintiff(s). Plaintiff and their counsel are committed to vigorously prosecuting this action on behalf of the members of the Class, and they have the resources to do so. Neither Plaintiff nor their counsel have any interest adverse to the interests of the other members of the Class.

59. **Superiority:** This class action is appropriate for certification because class proceedings are superior to other available methods for the fair and efficient adjudication of this controversy and joinder of all members of the Class is impracticable. This proposed class action presents fewer management difficulties than individual litigation, and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Class treatment will create economies of time, effort, and expense and promote uniform decision-making.

60. **Predominance:** Common questions of law and fact predominate over any questions affecting only individual Class members. Similar or identical violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action. For example, Defendant's liability and the fact of damages is common to Plaintiff and each member of the Class. If Defendant intercepted Plaintiff's and Class members' Website Communications, then Plaintiff and each Class member suffered damages by that conduct.

61. **Ascertainability:** Members of the Class are ascertainable. Class membership is defined using objective criteria and Class members may be readily identified through Defendant's books and records or the Session Replay Providers' books and records.

COUNT I
Violation of Illinois Eavesdropping Act

720 ILCS 5/14-1, *et seq.*

62. Plaintiff incorporates the preceding paragraphs as if fully set forth herein.

63. Plaintiff brings this claim individually and on behalf of the Class.

64. The Illinois Eavesdropping Act (the "Act") prohibits (1) using an eavesdropping device in a surreptitious manner to overhear, transmit, or record all or any part of any private conversation; (2) intercepting, recording, or transcribing, in a surreptitious manner, any private electronic communication without consent; (3) manufacturing, assembling, distributing, or possessing any electronic, mechanical, eavesdropping, or other device knowing that or having reason to know that the design of the device renders it primarily useful for the purpose of surreptitious overhearing, transmitting, or recording of private conversations or the intersection; or (4) using or disclosing any information which he or she knows or reasonably should know was obtained from a private conversation or private electronic communication without the consent of all parties to the private electronic communication. 720 ILCS 5/14-2.

65. Any party to any conversation or private electronic communication upon which eavesdropping was practiced shall be entitled to (1) an injunction to prohibit further eavesdropping; (2) actual damages; and (3) punitive damages. 720 ILCS 5/14-6.

66. "Eavesdropping device" is defined as any "any device capable of being used to hear or record oral conversation or intercept, or transcribe electronic communications whether such conversation or electronic communication is conducted in person, by telephone, or by any other means[.]" 720 ILCS 5/14-1(a).

67. "Eavesdropper" is defined as "any person, including any law enforcement officer and any party to a private conversation, who operates or participates in the operation of any eavesdropping device contrary to the provisions of this Article or who acts as a principal, as defined in this Article." 720 ILCS 5/14-1(b).

68. "Principle" is defined as "any person who: (1) knowingly employs another who illegally uses an eavesdropping device in the course of such employment; or (2) knowingly derives any benefit or information from the illegal use of an eavesdropping device by another; or (3) directs another to use an eavesdropping device illegally on his or her behalf." 720 ILCS 5/14-1(c).

69. "Private electronic communication" is defined as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or part by a wire, radio, pager, computer, electromagnetic, photo electronic or photo optical system, when the sending or receiving party intends the electronic communication to be private under circumstances reasonably justifying that expectation. A reasonable expectation shall include any expectation recognized by law, including, but not limited to, an expectation derived from a privilege, immunity, or right established by common law, Supreme Court rule, or the Illinois or United States Constitution." ILCS 5/14-1(e).

70. "Surreptitious" is defined as being "obtained or made by stealth or deception, or executed through secrecy or concealment." 720 ILCS 5/14-1(g).

71. Defendant is an "Eavesdropper" and "Principal" for purposes of the Act because it operates or participates in the operation of an eavesdropping device, knowingly employs another who illegally uses an eavesdropping device, derives a benefit or information from the illegal use of an eavesdropping device, and directs another to use an eavesdropping device illegally on its behalf.

72. Session Replay Code like that operated and employed at Defendant's direction is a "eavesdropping device" used to transcribe electronic communications within the meaning of the Act.

73. The Session Replay Providers are not a party to the Website Communications – Plaintiff and the Class only knew they were communicating with Defendant, not the Session Replay Providers.

74. Plaintiff's and Class members' intercepted Website Communications constitute the private electronic communications and private conversations within the meaning of the Act.

75. Defendant intentionally operated and employed Session Replay Code on its website to spy on, automatically and secretly, and intercept its website visitors' private electronic interactions communications with Defendant in real time.

76. Plaintiff's and Class members' private electronic communications were intercepted contemporaneously with their transmission.

77. Plaintiff and Class members had a reasonable expectation of privacy in their Website Communications based on the detailed information the Session Replay Code collected from Plaintiff and Class members.

78. Plaintiff and Class members did not consent to having their Website Communications surreptitiously intercepted and recorded.

79. Pursuant to 720 ILCS 5/14-6, Plaintiff and members of the Class are entitled to: (1) an injunction to prohibit further eavesdropping; (2) actual damages; and (3) punitive damages.

80. Defendant's conduct is ongoing, and it continues to unlawfully intercept the communications of Plaintiff and Class members any time they visit Defendant's website with Session Replay Code enabled without their consent. Plaintiff and Class members are entitled to declaratory and injunctive relief to prevent future interceptions of their communications.

COUNT II
Invasion of Privacy – Intrusion Upon Seclusion

81. Plaintiffs incorporate the preceding paragraphs as if fully set forth herein.

82. Plaintiffs bring this claim individually and on behalf of the Class.

83. Illinois common law recognizes the tort of invasion of privacy. The right to privacy is also embodied in the Illinois constitution.

84. Plaintiff and Class members had an objective, reasonable expectation of privacy in their Website Communications.

85. Plaintiff and Class members did not consent to, authorize, or know about Defendant's intrusion at the time it occurred. Plaintiff and Class members never agreed that Defendant could collect or disclose their Website Communications.

86. Plaintiff and Class members had an objective interest in precluding the dissemination and/or misuse of their information and communications and in conducting their personal activities without intrusion or interference, including the right to not have their personal information intercepted and utilized for business gain.

87. Defendant intentionally intruded on Plaintiff's and Class members' private life, seclusion, or solitude, without consent.

88. Defendant's conduct is highly objectionable to a reasonable person and constitutes an egregious breach of the social norms underlying the right to privacy.

89. Plaintiff and Class members were harmed by Defendant's wrongful conduct as Defendant's conduct has caused Plaintiff and the Class mental anguish and suffering arising from their loss of privacy and confidentiality of their electronic communications.

90. Defendant's conduct has needlessly harmed Plaintiff and the Class by capturing intimately personal facts and data in the form of their Website Communications. This disclosure and loss of privacy and confidentiality has caused Plaintiff and the Class to experience mental anguish, emotional distress, worry, fear, and other harms.

91. Additionally, given the monetary value of individual personal information, Defendant deprived Plaintiff and Class members of the economic value of their interactions with Defendant's website, without providing proper consideration for Plaintiff's and Class members' property.

92. Further, Defendant has improperly profited from its invasion of Plaintiff and Class members' privacy in its use of their data for its economic value.

93. As a direct and proximate result Defendant's conduct, Plaintiff and Class members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

94. Defendant's conduct is ongoing, and it continues to unlawfully intercept the communications of Plaintiff and Class members any time they visit Defendant's website with session replay software enabled without their consent. Plaintiff and Class members are entitled to declaratory and injunctive relief to prevent future interceptions of their communications.

REQUEST FOR RELIEF

Plaintiff, individually and on behalf of the other members of the proposed Class, respectfully requests that the Court enter judgment in Plaintiff's and the Class's favor and against Defendant as follows:

A. Certifying the Class and appointing Plaintiff as the Class representative;

B. Appointing Plaintiff's counsel as class counsel;

C. Declaring that Defendant's past conduct was unlawful, as alleged herein;

D. Declaring Defendant's ongoing conduct is unlawful, as alleged herein;

E. Enjoining Defendant from continuing the unlawful practices described herein, and awarding such injunctive and other equitable relief as the Court deems just and proper;

F. Awarding Plaintiff and the Class members statutory, actual, compensatory, consequential, punitive, and nominal damages, as well as restitution and/or disgorgement of profits unlawfully obtained;

G. Awarding Plaintiff and the Class members pre-judgment and post-judgment interest;

H. Awarding Plaintiff and the Class members reasonable attorneys' fees, costs, and expenses; and

I. Granting such other relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff, individually and on behalf of the Class, demands a trial by jury of any and all issues in this action so triable of right.

Dated: December 20, 2022

Respectfully Submitted,

By: */s/ Jason J. Kane*
Jason J. Kane
PEIFFER WOLF CARR KANE CONWAY & WISE LLP
95 Allens Creek Road
Building 1, Suite 150
Rochester, NY 14618
Ph: 585-310-5140
Email: jkane@peifferwolf.com

Brandon M. Wise – IL Bar # 6319580*
PEIFFER WOLF CARR KANE CONWAY & WISE LLP
818 Lafayette Ave., Floor 2
St. Louis, MO 63104
Ph: 314-833-4825
Email: bwise@peifferwolf.com
*to be admitted *pro hac vice*